UNITED STATES DISTRICT COURT
DISTRICT OF NEBRASKA

AMANDA BEASLEY, individually and on behalf of all others similarly situated, **Plaintiff,** **v.** **NELNET SERVICING, LLC,** **Defendant.**	**Case No.** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff AMANDA BEASLEY ("Plaintiff") brings this Class Action Complaint against NELNET SERVICING, LLC ("Defendant" or "Nelnet"), in her individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. This is a class action for damages with respect to Defendant Nelnet Servicing, LLC and it failure exercise reasonable care in securing sensitive personal information including without limitation, unencrypted and unredacted names, email addresses, phone numbers, and Social Security numbers (collectively, "personal identifiable information" or "PII").

2. Plaintiff seeks damages for herself and other similarly situated current and former student loan borrowers ("borrowers"), or any other person(s) impacted in the data breach at issue ("Class Members"), as well as other equitable relief, including, without limitation, injunctive relief designed to protect the very sensitive information of Plaintiff and other Class Members.

3. On or about August 26, 2022, Nelnet notified state Attorney Generals about a

widespread data breach involving sensitive PII of 2,501,324 individuals.[1] Nelnet explained in the required notice letter that it discovered an unauthorized third-party gained access to a portion of Nelnet's system. Nelnet discovered that files on its network were accessed and acquired by the unauthorized actor (the "Data Breach").

4. Plaintiff and the Class Members in this action were, upon information and belief, current and former student loan borrowers with their PII on Nelnet's system. Upon information and belief, the first that Plaintiff and the Class Members learned of the Data Breach was when they received by U.S. Mail Notice of Data Breach letters on August 26, 2022.

5. The Data Breach affected individuals whose information was stored on Defendants' servers in multiple states.

6. In this era of frequent data security attacks and data breaches, particularly in the financial industry, Defendant's failures leading to the Data Breach are particularly egregious, as this Data Breach was highly foreseeable.

7. Defendant reported to Plaintiff Amanda Beasley that information compromised in the Data Breach included her PII.

8. Upon information and belief, Plaintiff's and Class Members' PII was unencrypted and unredacted PII and was compromised due to Nelnet's negligent and/or careless acts and omissions.

9. Upon information and belief, based on the type of sophisticated and malicious criminal activity, the type of PII targeted, Defendant's admission that the PII was accessed, Defendants' admission that Plaintiffs and Class Member's PII was in the files that were accessed,

[1] Office of the Maine Attorney General, *Data Breach Notifications*, available at: https://apps.web.maine.gov/online/aeviewer/ME/40/f6b4d5be-f7ef-412b-9966-e323ad6443a0.shtml (last accessed August 29, 2022).

reports of criminal misuse of Plaintiffs' and Class Members' data, and reports of PII on the Dark Web following the Data Breach, Plaintiffs' and Class Members' PII was likely accessed, disclosed, exfiltrated, stolen, disseminated, and used by a criminal third party.

10. As a result of the Data Breach, Plaintiffs and the Class Members are at an imminent risk of identity theft.

11. The risk of identity theft is not speculative or hypothetical but is impending and has materialized as there is evidence that Plaintiffs' and Class Members' PII was targeted, accessed, and may have been disseminated on the Dark Web. Moreover, Class members have suffered actual identity theft and misuse of their data following the data breach.

12. As Defendant instructed, advised, and warned in its Notice Letters, Plaintiffs and the Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiffs' and Class Members' have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will include into the future: reviewing financial statements, changing passwords, and signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft.

13. Plaintiffs and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) invasion of privacy; (b) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time heeding Defendant's warnings and following its instructions in the Notice Letter; (g) the loss of benefit of the bargain (price premium damages), to the extent Class Members

paid AFR for services; (h) deprivation of value of their PII; and (i) the continued risk to their Sensitive Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Sensitive Information.

14. Plaintiffs seek to remedy these harms, and to prevent the future occurrence of an additional data breach, on behalf of themselves and all similarly situated persons whose PII was compromised as a result of the Data Breach. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement for loss of time, reimbursement of opportunity costs, out-of-pocket costs, price premium damages, and injunctive relief including improvements to Defendant's data security systems and protocols, future annual audits, and adequate credit monitoring services funded by the Defendant.

PARTIES

15. Plaintiff Amanda Beasley is a resident and citizen of Arkansas, residing in Vilonia. Ms. Beasley received Edfinancial's *Notice of Security Incident*, dated August 26, 2022, by U.S. Mail.

16. Defendant Nelnet Servicing, LLC is a Lincoln, Nebraska based student loan servicing company, which has a principal place of business at 121 S. 13TH Street, Suite 100, Lincoln, Nebraska 68508.

17. Defendant Nelnet Servicing, LLC is a wholly-owned subsidiary of Nelnet Diversified Solutions LLC, a Lincoln, Nebraska based limited liability company, which is itself a wholly-owned subsidiary of Nelnet Inc., a Lincoln, Nebraska based corporate conglomerate that deals in the administration and repayment of student loans and education financial services. Its principal place of business is located at 121 S. 13TH Street, Suite 100, Lincoln, Nebraska 68508.

18. All of Plaintiffs' claims stated herein are asserted against AFR and any of its

owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

19. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

20. The District of Nebraska has personal jurisdiction over Defendant named in this action because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in Nebraska and this District through its headquarters, offices, parents, and affiliates.

21. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Defendant's Promises

22. Defendant operates its business nationwide offering student loan services.

23. Plaintiff and the Class Members, as current or former student loan borrowers, reasonably relied (directly or indirectly) on this sophisticated student loan servicing company to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII. Borrowers, in general, demand security to safeguard their PII, especially when financial information and other sensitive PII is involved.

24. Indeed, NelNet promotes to its customer that it takes the privacy and security of PII seriously, stating, "The confidentiality, privacy, and security of our customers' information is one of our highest priorities."[2]

25. Defendant's Privacy Policy ("Privacy Policy") states, "Protecting your privacy is important to Nelnet and our employees ... We implement reasonable and appropriate physical, procedural, and electronic safeguards to protect your information."[3]

26. Defendant's Privacy Policy applies to any personal information provided to Nelnet and any personal information that Nelnet collects from its website, affiliates, and mobile apps.[4]

27. Defendant's Privacy Policy does not permit Defendant to use and disclose Plaintiff's and Class Members' Private Information unless complying with laws or to carry out internal functions.[5]

28. The Privacy Policy further states,

> Nelnet takes careful steps to safeguard customer information. We restrict access to your personal and account information to employees who need to know the information to provide services to you, and we regularly train our employees on privacy, information security, and their obligation to protect your information. We maintain reasonable and appropriate physical, electronic, and procedural safeguards to guard your Nonpublic Personal Information (NPI) and Personally Identifiable Information (PII), and we regularly test those safeguards to maintain the appropriate levels of protection.[6]

The Data Breach

29. Defendant violated its own Privacy Policy.

30. On August 26, 2022, Nelnet notified state Attorneys General ("AGs") and Class

---

[2] *Id.*
[3] https://www.nelnet.com/privacy-and-security
[4] *Id.*
[5] *Id.*
[6] *Id.*

Members about a widespread data breach of its computer network involving the sensitive personally identifiable information of consumers that impacted over 2million individuals.[7]

31. Beginning on or about August 26, 2022, Nelnet also sent affected persons (including Plaintiff Herrick) a written correspondence regarding the Data Breach, informing the recipients that their confidential data was involved.

32. According to its Notice Letters to Class Members, Nelnet explained it discovered on July 21, 2022 (over a full month earlier) that it detected an unauthorized third-party gained access to a portion of its information system and network. [8]

33. Nelnet "launched an investigation with third-party forensic experts" of Nelnet's systems, and determined that Plaintiff's and Class Members' personally identifiable information (including but not limited to full names and Social Security numbers) was present and likely stolen by the unauthorized person at the time of the incident.[9]

34. The letters Nelnet directed to be sent to borrowers of Edfinancial Services, LLC including Plaintiff and Class Members, noted unequivocally that their PII was impacted by the Data Breach.

35. Plaintiff and Class Members in this action were, upon information and belief, current and former student loan borrowers whose PII was utilized by Nelnet for purposes of servicing student loan payments. Plaintiff and Class Members first learned of the Data Breach when they received by U.S. Mail Notice of Data Breach letters dated August 26, 2022.

36. Upon information and belief, the PII was not encrypted prior to the Data Breach.

---

[7] https://apps.web.maine.gov/online/aeviewer/ME/40/f6b4d5be-f7ef-412b-9966-e323ad6443a0.shtml; https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-521.pdf.
[8] *Id.*
[9] *Id.*

Nelnet did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining, causing Plaintiff's and Class Members' PII to be exposed.

37. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII of Plaintiff and the Class Members.

Securing PII and Preventing Breaches

38. Nelnet could have prevented this Data Breach by properly encrypting or otherwise implementing policies, procedures and computer data security programs that provided the level of protection reasonably necessary for a company of this sophistication and the custodian of large amounts of PII.

39. In the course and scope of its student loan practices, Defendant collects massive amounts of highly sensitive PII, including but not limited to, names, email addresses, phone numbers, and Social Security numbers.

40. Collecting, maintaining, and protecting PII is vital to virtually all of Nelnet's business purposes, and Defendant benefits from the acquisition, use, and storage of the PII.

41. Plaintiffs and Class Members entrusted their PII to Defendants on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties, and/or only retain PII for necessary business purposes and for a reasonable amount of time.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

42. It is well known that PII, including Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

43. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Nelnet knew or should have known that its systems would be targeted by cybercriminals.

44. Indeed, cyberattacks against the financial industry have been common for over ten years with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cyber crime."[10]

45. Moreover, it is well known that the specific PII at issue in this case, including social security numbers and financial account information in particular, is a valuable commodity and a frequent target of hackers.

46. As a sophisticated financial and lending entity that collects, utilizes, and stores particularly sensitive PII, Nelnet was at all times fully aware of the increasing risks of cyber-attacks targeting the PII it controlled, and its obligation to protect the PII of Plaintiffs and Class

[10] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

Members.

47. Defendant has acknowledged through conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.

The Value of Personal Identifiable Information

48. There is both a healthy black market and a legitimate market for the type of PII that was compromised in this action. PII is such a valuable commodity to criminal networks that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

49. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the Dark Web. Numerous sources cite Dark Web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.

50. According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120. Criminals can also purchase access to entire company data breaches from $900 to $4,500.

51. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

52. A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.

53. The Social Security Administration has further warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, apply for a job using a false identity, open bank accounts, and apply for other government documents such as driver's license and birth certificates.

54. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

55. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

56. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

57. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card

information, personally identifiable information and Social Security Numbers are worth more than 10x in price on the black market."

Defendant Failed to Comply with Recognized Security Standards

58. Despite the prevalence of public announcements of data breach and data security compromises, and despite Defendant's own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and the proposed Class from being compromised.

59. Nelnet had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Nelnet breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

60. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

61. Upon information and belief, Defendant failed to comply with one or more of these standards.

Nelnet Failed to Comply with FTC Guidelines

62. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[11] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[12]

63. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

64. The FTC has brought well publicized enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. This includes the FTC's enforcement action against Equifax

[11] 17 C.F.R. § 248.201 (2013).
[12] *Id*.

following a massive data breach involving the personal and financial information of 147 million Americans.

65. In 2016, the FTC updated its publication, "Protecting Personal Information: A Guide for Business," which established cyber-security guidelines for businesses. There, the FTC advised that businesses should protect the PII that they keep by following some minimum standards related to data security, including, among others:

(a) Encrypting information stored on computer networks;

(b) Identifying network vulnerabilities;

(c) Implementing policies to update and correct any security problems;

(d) Utilizing an intrusion detection systems;

(e) Monitor all incoming traffic for suspicious activity indicating someone is attempting to hack the system;

(f) Watching for large amounts of data being transmitted from the system;

(g) Developing a response plan ready in the event of a breach;

(h) Limiting employee and vendor access to sensitive data;

(i) Requiting complex passwords to be used on networks;

(j) Utilizing industry-tested methods for security;

(k) Verifying that third-party service providers have implemented reasonable security measures;

(l) Educating and training employees on data security practices;

(m) Implementing multi-layer security including firewalls, anti-virus, and anti-malware software;

(n) Implementing multi-factor authentication.

66. Upon information and belief, Defendant failed to implement or adequately implement at least one of these fundamental data security practices.

67. Defendant's failure constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

Plaintiff and Class Members Have Suffered Concrete Injury as a Result of Defendant's Inadequate Security and the Data Breach it Allowed.

68. As a result of Defendant's ineffective and inadequate data security and retention measures, the Data Breach, and the foreseeable consequences of the PII ending up in the possession of criminals, the risk of identity theft is materialized and imminent.

69. Given the type of targeted attack in this case, the sophisticated criminal activity, and he type of PII, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/Dark Web for sale and purchase by criminals intending to utilize the PII for identity theft crimes, such as opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; or file false unemployment claims.

70. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts. The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

71. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. The fraudulent activity resulting from the Data Breach may not become evident for years.

72. Indeed, "[t]he risk level is growing for anyone whose information is stolen in a data breach." Javelin Strategy & Research, a leading provider of quantitative and qualitative research,

notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud." Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

73. To date, Defendant has done little to adequately protect Plaintiffs and Class Members, or to compensate them for their injuries sustained in this data breach.

74. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must, in Defendant's words, "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

75. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

76. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

77. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their

accounts, placing a credit freeze on their credit, and correcting their credit reports.

78. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendant or its clients for services, Plaintiffs and other reasonable consumers understood and expected that they were paying for services and data security, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected.

79. As a result of Defendant's ineffective and inadequate data security and retention measures, the Data Breach, and the imminent risk of identity theft, Plaintiffs and Class Members have suffered numerous actual and concrete injuries, including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) deprivation of value of their PII; and (i) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Sensitive Information.

Plaintiff Amanda Beasley's Experience

80. Plaintiff Beasley provided her personal information to Nelnet and/or its affiliate Edfinancial in conjunction with servicing related to student loan services Plaintiff obtained more than 14 years ago.

81. As part of her involvement with Defendant and Edfinancial, Plaintiff entrusted her

PII, and other confidential information such as name, address, Social Security number, phone number, financial account information, and other personally identifiable information to Defendant and Edfinancial with the reasonable expectation and understanding that they would at least take industry standard precautions to protect, maintain, and safeguard that information from unauthorized use or disclosure, and would timely notify her of any data security incidents related to her. Plaintiff would not have permitted her PII to be given to Nelnet had she known it would not take reasonable steps to safeguard her PII.

82. On or about August 26, 2022, nearly three months after Nelnet's breach began, Plaintiff Beasley received a letter from Nelnet notifying him that her PII had been improperly accessed and taken by unauthorized third parties. The notice indicated that Plaintiff Beasley's PII was compromised as a result of the Data Breach, despite the fact that her loans are long since paid and there is no reason for Nelnet to have retained her PII for so long.

83. As a result of the Data Breach, Plaintiff Beasley has or will make reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or personal records for any indications of actual or attempted identity theft or fraud.

84. Plaintiff spent this time at Defendant's direction. Indeed, in the Notice letter Plaintiff received, Defendant directed Plaintiff to take steps to mitigate her losses:

> We encourage you to remain vigilant against incidents of identity theft and fraud over the next 24 months, by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed "Steps You Can Take to Help Protect Your Personal Information."

85. Plaintiff Beasley suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Nelnet obtained from Plaintiff Beasley; (b) violation of her privacy rights; (c) the theft of her PII; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

86. As a result of the Data Breach, Plaintiff Beasley is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

87. The Data Breach has caused Plaintiff Beasley to suffer significant fear, anxiety, and stress, which has been compounded by the fact that Social Security number and other intimate details are in the hands of criminals.

88. As a result of the Data Breach, Plaintiff Beasley anticipates spending considerable time and/or money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Beasley will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

89. Plaintiff Beasley has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

90. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated.

91. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **All persons residing in the United States whose PII was compromised in the 2022 data breach announced by Nelnet Servicing, LLC in August 2022. (the "Nationwide Class").**

92. Excluded from the Classes are the following individuals and/or entities: Nelnet Servicing, LLC, and Nelnet's parents, subsidiaries, affiliates, officers and directors, and any entity in which Nelnet has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect

of this litigation, as well as their immediate family members.

93. Plaintiff reserves the right to modify or amend the definition of the proposed class and any future subclass before the Court determines whether certification is appropriate.

94. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are 2,501,324 individuals whose Private Information may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendant's records.

95. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exists and predominates over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect Plaintiff's and Class Members' PII;

b. Whether Defendant had duties not to disclose the Plaintiff's and Class Members' PII to unauthorized third parties;

c. Whether Defendant had duties not to use Plaintiff's and Class Members' PII for non-business purposes;

d. Whether Defendant failed to adequately safeguard Plaintiff's and Class Members' PII;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' PII;

k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

96. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

97. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

98. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

99. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

100. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered;

proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

101. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

102. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

103. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure and unlawful disclosure of the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

104. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

105. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise

due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether a contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that contract;

e. Whether Defendant breached the contract;

f. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

g. Whether Defendant breached the implied contract;

h. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

i. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information;

k. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

106. Plaintiff restates and realleges all of the foregoing paragraphs as if fully set forth herein.

107. As a condition of having their student loans processed, Plaintiff and Class Members, as current and former student loan borrowers, are obligated to provide Nelnet and/or its affiliates with certain PII, including but not limited to, their name, date of birth, address, Social Security number, state-issued identification numbers, tax identification numbers, military identification numbers, and financial account numbers.

108. Plaintiff and Class Members entrusted their PII to Nelnet and its affiliates on the premise and with the understanding that Nelnet would safeguard their information, use their PII for legitimate business purposes only, and/or not disclose their PII to unauthorized third parties.

109. Nelnet has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

110. Nelnet knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and/or using of the PII involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

111. Nelnet had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Nelnet's security protocols to ensure that Plaintiff's and Class Members' information in Nelnet's possession was adequately secured and protected.

112. Nelnet also had a duty to have procedures in place to detect and prevent the

improper access and misuse of Plaintiff's and Class Members' PII.

113. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of Nelnet's business as sophisticated student loan service provider, for which the diligent protection of PII is a continuous forefront issue.

114. Plaintiff and Class Members were the foreseeable and probable victims of Nelnet's inadequate security practices and procedures. Nelnet knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Nelnet's systems.

115. Nelnet's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Nelnet's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Nelnet's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' PII, including basic encryption techniques freely available to Nelnet.

116. Plaintiff and Class Members had no ability to protect their PII that was in, and possibly remains in, Nelnet's possession.

117. Nelnet was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

118. Nelnet had and continues to have a duty to adequately and promptly disclose that Plaintiff's and Class Members' PII within Nelnet's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

119. Nelnet had a duty to employ proper procedures to prevent the unauthorized dissemination of Plaintiff's and Class Members' PII.

120. Nelnet has admitted that the PII of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

121. Nelnet, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII during the time the PII was within Nelnet's possession or control.

122. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

123. These foregoing frameworks are existing and applicable industry standards in the financial services industry, and Defendant failed to comply with these accepted standards thereby opening the door to the cyber incident and causing the data breach.

124. Nelnet improperly and inadequately safeguarded Plaintiff's and Class Members' PII in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

125. Nelnet failed to heed industry warnings and alerts to provide adequate safeguards to protect borrower PII in the face of increased risk of theft.

126. Nelnet, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and

prevent dissemination of the PII.

127. Nelnet, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

128. But for Nelnet's wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' PII would not have been compromised.

129. There is a close causal connection between Nelnet's failure to implement security measures to protect Plaintiff's and Class Members' PII and the harm suffered or risk of imminent harm suffered by Plaintiff and Class. Plaintiff's and Class Members' PII was lost and accessed as the proximate result of Nelnet's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

130. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Nelnet, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Nelnet's duty in this regard.

131. Nelnet violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Nelnet's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

132. Nelnet's violation of Section 5 of the FTC Act constitutes negligence *per se*.

133. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

134. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class.

135. As a direct and proximate result of Nelnet's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Nelnet's possession and is subject to further unauthorized disclosures so long as Nelnet fails to undertake appropriate and adequate measures to protect the PII in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of Nelnet's goods and services they received.

136. As a direct and proximate result of Nelnet's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

137. Additionally, as a direct and proximate result of Nelnet's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remains in Nelnet's possession and is subject to further unauthorized disclosures so long as Nelnet fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT II
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

138. Plaintiff restates and realleges all of the foregoing paragraphs as if fully set forth herein.

139. Plaintiff and Class Members conferred a monetary benefit on Defendant and its affiliate student loan companies in the form of monetary payments—directly or indirectly—for providing student loan services to current and former borrowers.

140. Defendant collected, maintained, and stored the PII of Plaintiff and Class Members and, as such, Defendant had knowledge of the monetary benefits it received on behalf of the Plaintiff and Class Members.

141. The money that borrowers paid to Defendant should have been used to pay, at least in part, for the administrative costs and implementation of data security adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII.

142. Defendant failed to implement—or adequately implement—those data security practices, procedures, and programs to secure sensitive PII, as evidenced by the Data Breach.

143. As a result of Defendant's failure to implement data security practices, procedures, and programs to secure sensitive PII, Plaintiff and Class Members suffered actual damages in an

amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiff's PII.

144. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement the data security measures adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII and that the borrowers paid for.

145. As a direct and proximate result of Defendant's decision to profit rather than provide adequate security, and Defendant's resultant disclosures of Plaintiff's and Class Members' PII, Plaintiff and Class Members suffered and continue to suffer considerable injuries in the forms of time and expenses mitigating harms, diminished value of PII, loss of privacy, and a present increased risk of harm.

COUNT III
Breach of Express Contract
(On Behalf of Plaintiff and the Nationwide Class)

146. Plaintiff restates and realleges all of the foregoing paragraphs as if fully set forth herein.

147. This count is plead in the alternative to Count II (Unjust Enrichment) above.

148. Plaintiff and Class Members allege that they were the express, foreseeable, and intended beneficiaries of valid and enforceable express contracts between Defendant and its former and current customers, contract(s) that (upon information and belief) include obligations to keep sensitive PII private and secure.

149. Upon information and belief, these contracts included promises made by Defendant that expressed and/or manifested intent that the contracts were made to primarily and directly benefit the Plaintiff and the Class (all customers entering into the contracts), as Defendant's service

was for student loan services for Plaintiff and the Class, but also safeguarding the PII entrusted to Defendant in the process of providing these services.

150. Upon information and belief, Defendant's representations required Defendant to implement the necessary security measures to protect Plaintiff's and Class Members' PII.

151. Defendant materially breached its contractual obligation to protect the PII of Plaintiff and Class Members when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

152. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

153. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure of their PII, the loss of control of their PII, the present risk of suffering additional damages, and out-of-pocket expenses.

154. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

155. Plaintiff re-alleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

156. This count is plead in the alternative to Count II (Unjust Enrichment) above.

157. Plaintiff's and Class Members' PII was provided to Defendant as part of student loan services that Defendant provided to Plaintiff and Class Members.

158. Plaintiff and Class Members agreed to pay Defendant for its services.

159. Defendant and the Plaintiff and Class Members entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning the security of Plaintiff's and Class Members' PII, whereby, Defendant was obligated to take reasonable steps to secure and safeguard Plaintiff's and Class Members' PII.

160. Defendant had an implied duty of good faith to ensure that the PII of Plaintiff and Class Members in its possession was only used in accordance with its contractual obligations.

161. Defendant was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiff's and Class Members' PII and to comply with industry standards and applicable laws and regulations for the security of this information.

162. Under these implied contracts for data security, Defendant was further obligated to provide Plaintiff and all Class Members, with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII.

163. Defendant breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiff's and Class Members' PII, resulting in the Data Breach.

164. Defendant further breached the implied contract by providing untimely notification to Plaintiff and Class Members who may already be victims of identity fraud or theft or are at present risk of becoming victims of identity theft or fraud.

165. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

166. As a result of Defendant's conduct, Plaintiff and Class Members did not receive the full benefit of the bargain.

167. Had Defendant disclosed that its data security was inadequate, neither the Plaintiff or Class Members, nor any reasonable person would have entered into such contracts with Defendant.

168. As a result of Data Breach, Plaintiff and Class Members suffered actual damages resulting from the theft of their PII, as well as the loss of control of their PII, and remain at present risk of suffering additional damages.

169. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

170. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT V
Invasion of Privacy
(On Behalf of Plaintiff and the Nationwide Class)

171. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

172. Plaintiff and Class Members have a legally protected privacy interest in their PII, which is and was collected, stored, and maintained by Defendant, and they are entitled to the reasonable and adequate protection of their PII against foreseeable unauthorized access and publication of their PII to criminal actors, as occurred with the Data Breach. The PII of Plaintiff and Class Members contain intimate details of a highly personal nature, individually and in the aggregate.

173. Plaintiff and Class Members reasonably expected that Defendant would protect and secure their PII from unauthorized parties and that their PII would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

174. Defendant intentionally intruded into Plaintiff's and Class Members' seclusion by disclosing without permission their PII to a third party.

175. By failing to keep Plaintiff's and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, inter alia:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their PII obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to adequately secure their PII from disclosure to unauthorized persons; and

d. enabling the disclosure of their PII without consent.

176. This invasion of privacy resulted from Defendant's intentional failure to properly secure and maintain Plaintiff's and Class Members' PII, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

177. Plaintiff and Class Members' PII is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiff's, and Class Members' PII, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

178. The disclosure of Plaintiff's and Class Members' PII to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

179. Defendant's willful and reckless conduct that permitted unauthorized access, exfiltration and disclosure of Plaintiff's and Class Members' intimate and sensitive PII is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

180. The unauthorized access, exfiltration, and disclosure of Plaintiff's and Class Members' PII was without their consent, and in violation of various statutes, regulations and other laws.

181. As a direct and proximate result of Defendant's intrusion upon seclusion, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seek an award of nominal damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against Nelnet Servicing, LLC and that the Court grant the following:

A. For an Order certifying the Nationwide Classes and appointing Plaintiff and his Counsel to represent the certified Nationwide Class;

B. For equitable relief enjoining Nelnet from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to the Plaintiff and Class;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including

but not limited to an order:

i. prohibiting Nelnet from engaging in the wrongful and unlawful acts described herein;

ii. requiring Nelnet to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Nelnet to delete, destroy, and purge the personal identifying information of Plaintiff and Class unless Nelnet can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class;

iv. requiring Nelnet to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and Class Members' personal identifying information;

v. prohibiting Nelnet from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring Nelnet to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Nelnet's systems on a periodic basis, and ordering Nelnet to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Nelnet to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Nelnet to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Nelnet to segment data by, among other things, creating firewalls and access controls so that if one area of Nelnet's network is compromised, hackers cannot gain access to other portions of Nelnet's systems;

x. requiring Nelnet to conduct regular database scanning and securing checks;

xi. requiring Nelnet to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Nelnet to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Nelnet to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Nelnet's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Nelnet to implement, maintain, regularly review, and

revise as necessary a threat management program designed to appropriately monitor Nelnet's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Nelnet to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Nelnet to implement logging and monitoring programs sufficient to track traffic to and from Nelnet's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Nelnet's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: September 2nd, 2022

Respectfully Submitted,

/s/ *Gary M. Klinger*
Gary M. Klinger
David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
Fax: (865) 522-0049
gklinger@milberg.com
dlietz@milberg.com

Joseph M. Lyon (*pro hac vice* forthcoming)
THE LYON FIRM, LLC
2754 Erie Ave.
Cincinnati, OH 45208
Phone: (513) 381-2333
jlyon@thelyonfirm.com
cwatson@thelyonfirm.com

Attorneys for Plaintiff and the Proposed Class